Guía de respuesta a una infección por *malware*

ENJOY SAFER TECHNOLOGY™

Contenido

1. Introducción

En la actualidad, una de las principales causas de incidentes de seguridad son los códigos maliciosos o *malware* (por la contracción de las palabras en inglés *malicious software*), un término que incluye a todo aquel *software* que tiene como propósito afectar la información o bien los sistemas que la procesan, almacenan y transmiten.

Las razones de la incidencia del *malware* están relacionadas con su incremento, que considera principalmente tres variables: cantidad, complejidad y diversidad. En cuanto a la cantidad, los laboratorios de ESET a nivel mundial reciben alrededor de 200 mil nuevas variantes de códigos maliciosos por día, lo que permite tener una idea de la afectación que podrían padecer los usuarios y las empresas.

De la misma manera, cada vez se desarrollan programas dañinos de mayor complejidad en comparación con los primeros tipos de *malware*. Por ejemplo, los mecanismos utilizados actualmente por distintas versiones de programas maliciosos hacen muy difícil la recuperación de la información una vez que ha sido afectada. Un ejemplo de esto son ciertas variantes de *ransomware* que cifran archivos o bloquean sistemas, utilizando complejos protocolos, que una vez infectados son prácticamente irrecuperables, a menos que se tenga un *backup* o se pague el rescate monetario que exigen los ciberdelincuentes, una acción que no es recomendable en ningún caso.

En lo que a la diversidad se refiere, las distintas familias de códigos maliciosos y sus variantes han evolucionado para afectar un conjunto amplio de artefactos utilizados actualmente, desde computadoras, dispositivos móviles (*smartphones* o tabletas), terminales de punto de venta (*PoS*) o aparatos inteligentes como televisores, hasta los denominados *wearables* o dispositivos 'usables', como los *smartwatches*.

Sin duda, se trata de una amenaza latente que seguramente continuará creciendo, con métodos de infección cada vez más sofisticados, lo que se traduce en retos para la protección de la información en las empresas, y en una perspectiva a largo plazo, se trata de nuevos desafíos para la protección de los negocios.

Por lo anterior, resulta necesario conocer la manera de atender estas incidencias, como una de las funciones relevantes de los equipos de seguridad dentro de las organizaciones, razón por la cual el presente documento pretende ser una guía general sobre las acciones a seguir antes, durante y después de un incidente relacionado con algún tipo de programa malicioso.

Esta guía también incluye una sección sobre los tipos de *malware* detectados con mayor frecuencia, mostrando sus principales características y diferencias. Además, considera las principales tendencias en materia de propagación e infección de estas amenazas, así como recomendaciones para enfrentar de manera proactiva y reactiva ataques por códigos maliciosos, junto con procedimientos para el envío de muestras al Laboratorio de análisis e investigación de ESET Latinoamérica.

1.1. Conceptos generales y tipos de *malware*

Generalmente, cuando un programa malicioso infecta un sistema, se suele hacer referencia a un "virus", sin embargo, puede tratarse de cualquier otro tipo de *malware*. De hecho, actualmente solo un bajo porcentaje de los códigos maliciosos que se desarrollan y propagan por Internet corresponde a los denominados virus.

En su lugar, otros tipos de *malware* han proliferado para afectar a los usuarios con nuevas y variadas técnicas de propagación e infección, mismos que pueden ser clasificados en función de sus características, propósitos o funcionalidades. Con el objetivo de tener más información al respecto, en los siguientes párrafos se describen los tipos de *malware* más comunes.

Quizá la categoría de *malware* más conocida efectivamente corresponda a los virus, que obtuvieron su nombre luego de una analogía con los virus biológicos que solo pueden reproducirse dentro de las células de otros organismos, tal como lo hacen los virus informáticos, que requieren un archivo huésped para infectar a un equipo.

Sin embargo, existen amenazas como los gusanos que, a diferencia del virus, no requieren un archivo anfitrión y tienen la capacidad de replicarse y propagarse por sí mismos; o los troyanos, que simulan ser una aplicación inofensiva o benévola, pero que en realidad realizan tareas maliciosas sin el consentimiento y muchas veces sin el conocimiento del usuario.

Los *rootkits* son otro tipo de programa malicioso que garantiza a los atacantes el acceso a un sistema, a la vez que ocultan su presencia. Luego de acceder, generalmente debido a una vulnerabilidad, utilizan funciones del sistema operativo para evitar ser detectados: ocultan procesos, archivos o registros, por lo que es difícil detectarlos por medio de técnicas convencionales de seguridad.

También es posible encontrar otros tipos de *malware*, como el *spyware*, que recopila información de las actividades de los usuarios y la envía a un atacante, o las *botnets*, redes de equipos infectados (conocidos como zombis o *bots*) que permiten a un cibercriminal utilizarlos, de forma remota, con diversos fines, como propagar más códigos maliciosos, emplearlos para ataques de Denegación de Servicio (*DoS* por sus siglas en inglés, *Denial of Service*) o utilizarlos para enviar correos no deseados de forma masiva (*spam*), por citar algunos ejemplos.

Con la evolución de los códigos maliciosos se han desarrollado amenazas de mayor complejidad; en este sentido, se han registrado subcategorías de troyanos como es el caso de *downloaders* (que permiten descargar otras amenazas desde Internet para instalarlas posteriormente), *droppers* (que instalan otros programas maliciosos incluidos en su código fuente), *clickers* (para generar tráfico hacia sitios o avisos publicitarios que generan ganancias a sus desarrolladores) o los que se incluyen en la categoría de bancarios, creados especialmente para obtener datos relacionados con entidades financieras.

Asimismo, una tendencia creciente es el desarrollo de programas maliciosos que buscan generar un beneficio económico para sus desarrolladores con mayor rapidez. Tal es el caso del *ransomware*, un tipo de *malware* que cifra la información o bloquea un sistema para impedir el acceso a los datos. Posteriormente, solicita un pago como rescate, para que el atacante pueda proporcionar la clave que permite al usuario acceder a los archivos "secuestrados". Cabe destacar que el pago no garantiza que los datos puedan ser restablecidos.

Como se observa, la gama de amenazas informáticas es amplia, compleja y cada vez más diversa, ya que ahora no solamente es posible encontrar *software* malicioso para los equipos de cómputo tradicionales; los teléfonos inteligentes también se han visto afectados por programas y aplicaciones que tienen como propósito generar un daño patrimonial a los usuarios, especialmente sobre las plataformas móviles más utilizadas. En fechas recientes, también se han visto afectados otros dispositivos, como *SmartWatch* o *SmartTV*, que funcionan a partir de un sistema operativo, lo que apunta al desarrollo de amenazas hacia la Internet de las Cosas (*IoT* por sus siglas en inglés).

1.2. Aplicaciones potencialmente indeseables (PUAS)

Además de los códigos maliciosos, es posible identificar otro tipo de programas que también pueden afectar a los usuarios y que por su naturaleza alcanzan otra clasificación. Se trata de las PUAS, acrónimo de *Potentially Unwanted Application*, es decir, una aplicación potencialmente indeseada.

Este tipo de programas informáticos presentan un comportamiento probablemente indeseado por el usuario, que por lo general no exhiben el comportamiento típico del *malware* y requieren del consentimiento del usuario antes de realizar la instalación (*User License Agreement*).

Sin embargo, realizan otro tipo de acciones, como instalar aplicaciones adicionales, cambiar el comportamiento del entorno donde se ejecutó, instalar algún tipo de *adware* sin advertirlo para mostrar publicidad no solicitada, modificar configuraciones de los navegadores o instalar barras de herramientas (*toolbars)*.

En las soluciones de seguridad de ESET la detección de una PUA es opcional; en caso de que el usuario requiera identificar las aplicaciones potencialmente indeseables, en la solución contra *malware* se debe elegir la activación de esta funcionalidad durante el proceso de instalación del producto, ya que por defecto se encuentra desactivada.

Por lo tanto, utilizando los ajustes predeterminados de las soluciones de seguridad de ESET no se eliminarán las PUAS como parte de la exploración. Si bien el usuario puede ser notificado cuando este tipo de aplicaciones se encuentran instaladas en el sistema, es necesario habilitar la opción 'Desinfección estricta' para que el producto de ESET las elimine de forma automática.

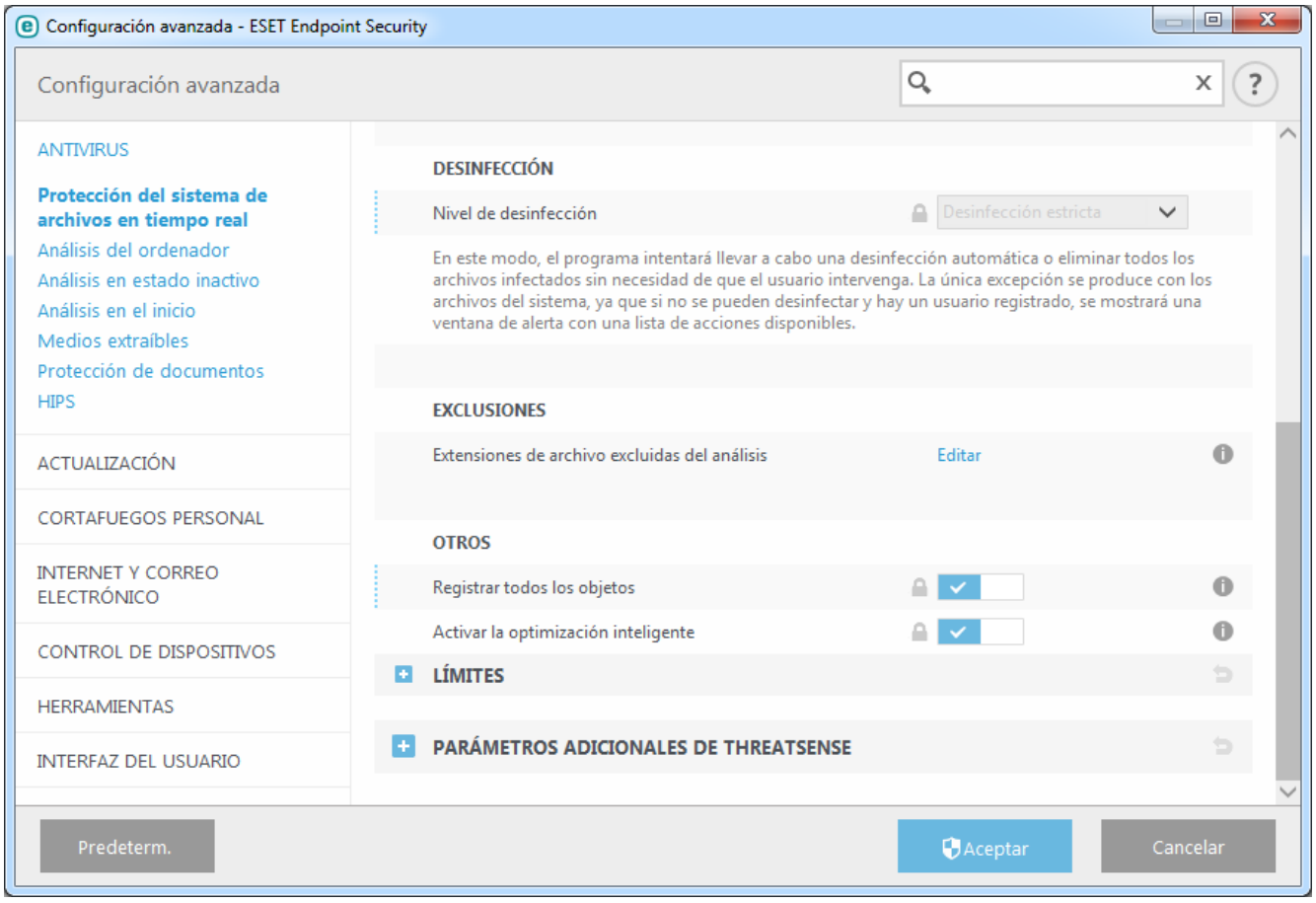

Imagen 1. Interfaz de configuración avanzada de ESET Endpoint Security para nivel de desinfección estricta.

1.3. Aplicaciones Potencialmente Peligrosas

También existen otros programas cuya función es simplificar la administración de equipos en red, incluso algunos que se distribuyen como *software* comercial legítimo. Sin embargo, debido a sus funcionalidades y características pueden ser utilizados con propósitos maliciosos. Las denominadas 'Aplicaciones Potencialmente Inseguras' (*Possible Unsafe Application*) es el término utilizado para este tipo de *software*.

Pueden incluir programas como herramientas de acceso remoto, aplicaciones para adivinar contraseñas o registradores de pulsaciones en el teclado. A través de las soluciones de seguridad es posible detectarlos, y de la misma manera que las aplicaciones potencialmente indeseables, los parámetros pueden ser configurados para la detección de este tipo de programas ya sea desde la instalación o posterior a ella.

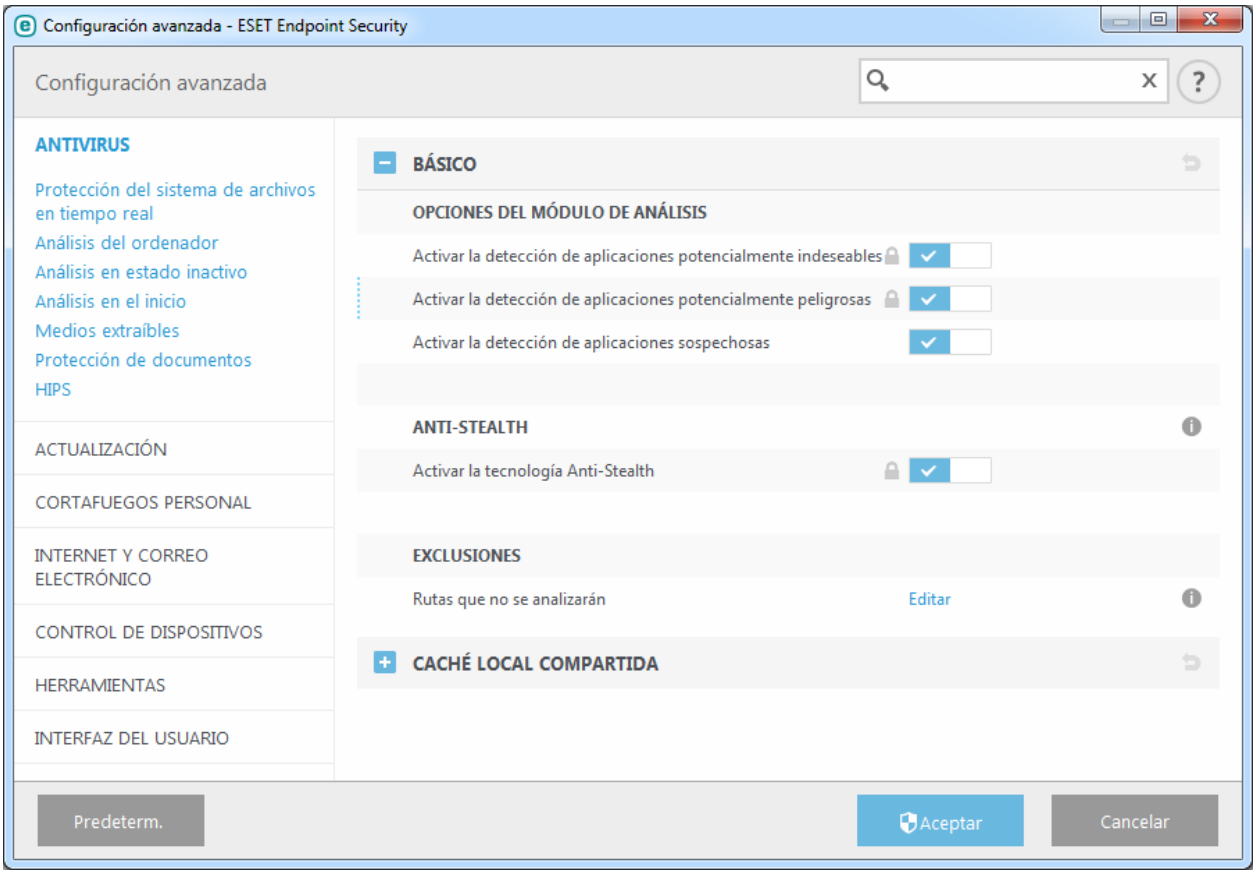

Imagen 2. Interfaz de configuración avanzada de ESET Endpoint Security para diferentes tipos de aplicaciones.

1.4. Tendencias del *software* malicioso en Latinoamérica

Como se mencionó anteriormente, el malware ha pasado de los tradicionales y más conocidos virus, a un conjunto de programas maliciosos con una mayor tasa de propagación. Por ejemplo, las *botnets* han sido desde hace varios años una de las principales amenazas utilizadas por los cibercriminales, y es posible pronosticar que esta tendencia se mantendrá.

Además, en los últimos años hemos sido testigos de un aumento considerable en las infecciones por *cripto ransomware*, con distintas familias de los denominados *filecoders* (detectados por los productos de ESET como variantes de *Win32/FileCoder*) y *lockscreens*, que bloquean el acceso a los sistemas. Estos programas no solo afectan a los equipos de escritorio, sino que además se han creado para plataformas móviles como Android y, recientemente, para dispositivos vinculados con la *IoT*.

De acuerdo con el informe *ESET Security Report Latinoamérica 2015*, un estudio sobre las tendencias de seguridad con base en encuestas a administradores de sistema y ejecutivos de las principales empresas de Latinoamérica, la infección por códigos maliciosos es la primera causa de incidentes de seguridad. Sin importar si se trata de organizaciones pequeñas, medianas o grandes, los ciberdelincuentes las afectan de igual manera, incluso con ataques dirigidos.

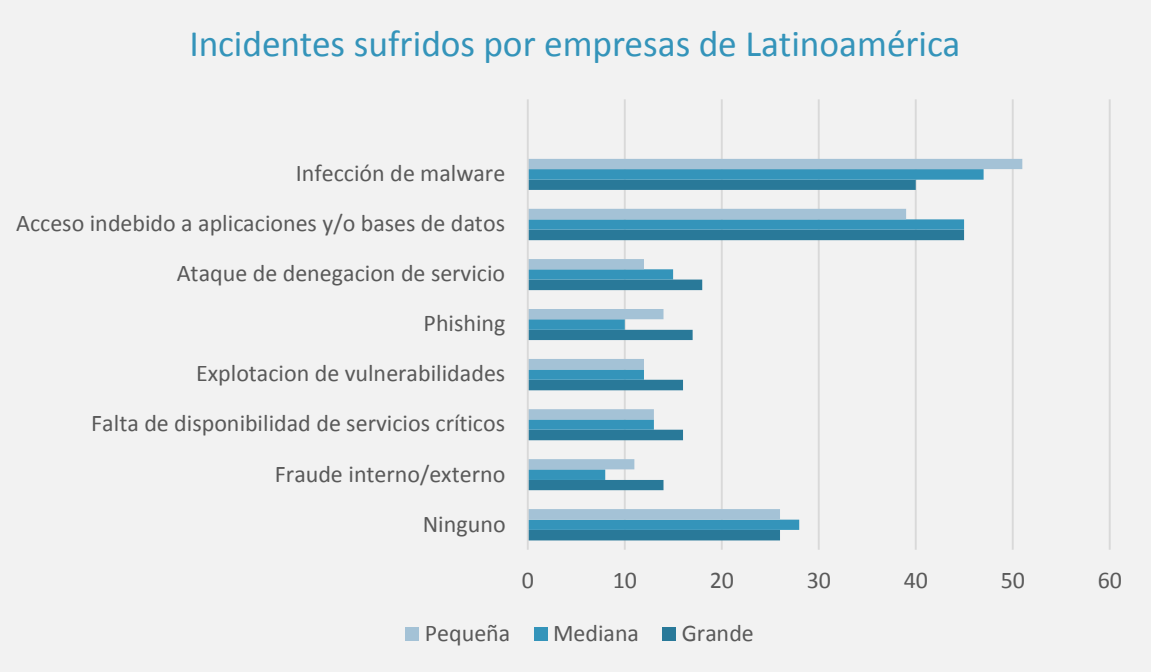

Imagen3. Porcentaje de incidentes de seguridad padecidos por empresas latinoamericanas.

Los resultados indican que, en promedio, la mitad de los encuestados señalaron haber sido afectados por algún tipo de *malware*. Las consecuencias de una infección varían en función del código malicioso en cuestión, que pueden ir desde espiar la actividad de los usuarios, robo y secuestro de información, hasta daños a la infraestructura tecnológica de la organización.

No obstante, existen consecuencias más graves derivadas de un incidente, como la fuga de información o la filtración de datos de usuarios y clientes, casos que dañan seriamente la imagen y reputación de las organizaciones. Por estas razones, resulta fundamental proteger la información y el negocio desde todos los frentes de ataque posibles.

2. Riesgos de seguridad asociados a los códigos maliciosos

2.1. Síntomas comunes de una infección por *malware*

Actualmente, la gran mayoría del *software* de seguridad contra códigos maliciosos permite identificar un porcentaje muy elevado de este tipo de amenazas informáticas. Sin embargo, en ausencia de estas soluciones existen altas posibilidades de padecer un incidente por *malware*, ya sea por falta de actualización del *software*, una configuración errónea o malas prácticas aplicadas a la Seguridad Informática.

Ante la falta de herramientas que permitan detectar de manera automática una infección por *malware*, existen distintos indicios que podrían mostrar que un sistema no está funcionando de la manera en la que debería. Esto representa una dificultad para saber de manera precisa si se está ante una infección, puesto que la mayoría de las amenazas buscan pasar inadvertidas. Sin embargo, esto no aplica en todos los casos, ya que existe *malware* que se hace evidente al usuario cuando infecta su equipo.

A pesar de ello, a continuación se presentan algunos "síntomas" de una posible infección:

- Bajo desempeño en el procesamiento de tareas en el equipo.
- Aparición de ventanas y anuncios emergentes que no han sido solicitadas por el usuario.
- Aparición de programas instalados en el equipo sin el conocimiento y consentimiento del usuario.
- Comportamiento anormal del sistema operativo, como reinicio o apagado repentino.
- Fallas durante la descarga de actualizaciones del sistema operativo o de programas instalados.
- Funcionalidades deshabilitadas del sistema operativo o de programas.
- Lentitud al navegar por Internet o durante la descarga de archivos.
- Alertas de seguridad por parte del sistema operativo o de supuestas soluciones antivirus.
- Imposibilidad de iniciar el sistema operativo tanto en "modo normal" como en "modo seguro".
- Cambio de página de inicio de Internet o redirección a sitios web desconocidos.
- Cambio del fondo de escritorio u otro aspecto del sistema.
- Mensajes intimidatorios para el usuario o solicitud de pagos para recuperar información.
- Conexiones de red entrantes y salientes por puertos y protocolos comúnmente no utilizados.

De manera general, este tipo de comportamientos podrían determinar que uno o más equipos se encuentran infectados. Ante las dudas, el método más fehaciente es el análisis y exploración que pueda realizar una solución de seguridad contra códigos maliciosos.

2.2. Riesgos de seguridad asociados al *malware*

Relacionados con una infección, existen una infinidad de riesgos de seguridad asociados con los códigos maliciosos, mismos que varían de acuerdo con la intención de sus desarrolladores, que pueden ir desde robar o dañar información, hasta afectar los sistemas, equipos o redes.

De manera general, un programa puede ser calificado como malicioso si el *software* monitorea la actividad y el comportamiento del usuario sin su conocimiento (y probablemente contra su voluntad), modifica la información o impide el acceso a ella. En otras palabras, todo aquel programa que atenta contra la confidencialidad, integridad o disponibilidad de la información perteneciente a los usuarios u organizaciones debe ser identificado como *malware*.

Por ello, más allá del robo de información sensible, las consecuencias derivadas de una afectación a alguna de las propiedades de los datos antes mencionadas, pueden magnificar los efectos negativos. Además, es preciso tener en cuenta el país o la industria a la que pertenece la empresa afectada, dado que un incidente de seguridad y/o la fuga de información podrían tener un impacto aún mayor en su reputación e imagen, incluso con implicaciones legales si se debe cumplir con alguna legislación, contrato o regulación.

2.3. Riesgos de seguridad relacionados con las PUAS

En el mismo sentido, las cuestiones relacionadas a la detección de las PUAS radican también en otros aspectos más allá de lo estrictamente técnico. Por ejemplo, es importante determinar si la aplicación en cuestión es realmente legítima o no, con base en la intención de sus desarrolladores, los posibles temas legales y éticos que conllevan detectar este tipo de programas.

Para poder establecer un criterio sobre qué tan malicioso es un *software* y si reúne los antecedentes necesarios para que entre en la categoría de PUA, deben considerarse diversos factores, como las funciones y utilidad que le otorgan al usuario, el modelo o canal de distribución a través del cual se obtiene la misma y la potencial amenaza que pueda presentar para el entorno informático en cuanto a la Seguridad de la Información y la estabilidad de los sistemas.

Debido a lo anterior, las decisiones se deben tomar en concordancia con las políticas de seguridad en las organizaciones y optar por definir si las funcionalidades de una aplicación potencialmente indeseable y peligrosa superan los riesgos asociados a esta categoría de programas. Por tal razón, las soluciones de ESET permiten activar o desactivar por separado ambas opciones. La configuración se puede gestionar de manera centralizada a través de *ESET Remote Administrator*, la consola de administración remota de ESET.

3. ¿Qué hacer en caso de una infección por *malware*?

Utilizando como referencia nuevamente el *ESET Security Report 2015*, es estudio muestra que la mayor cantidad de incidentes de seguridad en las organizaciones están relacionados con afectaciones por códigos maliciosos. Distintos síntomas pueden ser identificados para determinar que un equipo o un conjunto de ellos han sido infectados por algún tipo de *malware*, ya sea de manera manual o automatizada con alguna solución de seguridad.

Por ello, resulta muy importante conocer las acciones a seguir si se ha determinado que uno o más equipos han sido afectados. Si bien no se trata de una guía definitiva y exhaustiva sobre lo que se tiene que realizar en caso de una infección por *malware*, los siguientes pasos permitirán definir fases y estimar recursos necesarios para atender una incidencia de esta naturaleza. Del mismo modo, pueden formar parte de un **Plan de Respuesta a Incidentes de Seguridad** o IRP por sus siglas en inglés.

Este documento considera un conjunto de fases que, al igual que un IRP (*Incidente Response Plan*), definen actividades y funciones básicas para hacer frente a algún incidente que comprometa la Seguridad de la Información, y sobre la manera de proceder ante los diferentes escenarios en los cuales podrían estar expuestos los activos de la organización si algún riesgo se materializa.

Debido a la naturaleza de las amenazas, existe la probabilidad de padecer las consecuencias de un incidente, incluso a veces contando con controles de seguridad implementados y en operación. Por tanto, estos planes se consideran actividades preventivas y reactivas, de manera que puedan evitarse las infecciones por *malware* o, en su defecto, que de presentarse sus consecuencias sean las mínimas aceptables.

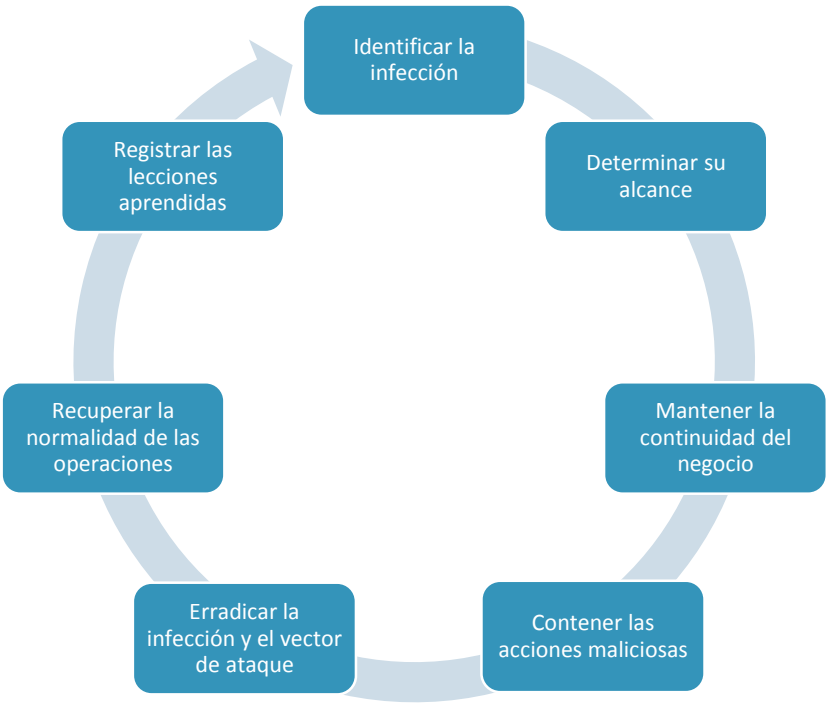

Imagen 4. Fases para atender un incidente de infección por malware.

El propósito primordial consiste en mantener el número de incidentes en un nivel razonablemente bajo para proteger los procesos de negocio críticos de la organización. Cuando se trata de incidentes relacionados con *malware*, se pueden seguir actividades que contribuyen a una efectiva respuesta y rápida recuperación.

3.1. Identificar la infección

Un incidente de seguridad relacionado con *malware* puede ser detectado de diferentes maneras y con distintos niveles de detalle, y para hacerlo se pueden utilizar desde herramientas de detección automatizadas -como consolas que centralizan la información relacionada con amenazas identificadas en los equipos administrados- hasta medios manuales -como un reporte de falla de un usuario que considere un comportamiento anormal en su sistema.

Algunos incidentes muestran signos que facilitan la detección, no obstante, se pueden presentar ocasiones en donde es casi imposible detectarlos si no se cuenta con herramientas adecuadas. Por lo tanto, reconocer los indicios de infección es fundamental para conocer los equipos infectados y la información que puede estar en riesgo. Familias de *malware* han cambiado su funcionamiento tradicional que buscaba pasar desapercibido al usuario; otras familias, por el contrario, se han vuelto muy evidentes para mostrar que han afectado los equipos o la información, tal es el caso del *ransomware*.

Las actividades de detección de *malware* pueden aplicarse a distintos niveles dentro de la organización: a nivel de *host* (en los sistemas operativos de servidores y estaciones de trabajo), a nivel de aplicaciones de servidor (correo electrónico o *proxies web*) y a nivel de aplicaciones de cliente (mensajería instantánea o correo electrónico de clientes). Independientemente de la manera en la cual se lleve a cabo, la detección es el paso inicial para atender un incidente por *malware*.

3.2. Determinar el alcance de la infección

Luego de la identificación de una infección por *malware*, es necesario determinar la cantidad de sistemas que han sido comprometidos y de qué manera, con el propósito de conocer el alcance de la infección y el impacto que puede representar. Por ejemplo, si está limitada a un único equipo, un conjunto de ellos, una subred o, en casos más graves, a toda la red corporativa.

Conocer el alcance de una infección permite calcular los recursos que serán necesarios para solucionar los inconvenientes que haya generado. Además, permite saber los sistemas que han sido comprometidos, junto con la criticidad de la información que almacenan, procesan o transmiten.

Por otro lado, a partir del tipo de *malware* y su comportamiento, también es posible determinar saber si se ha filtrado información sensible, si se han visto comprometidos datos corporativos o privados de los empleados y/o de clientes. En general, es necesario identificar la información y los sistemas que han sido dañados para estimar las consecuencias negativas.

3.3. Mantener la continuidad del negocio

Durante un incidente, resulta fundamental mantener la continuidad de las operaciones críticas de las organizaciones. En el caso de incidentes por *malware*, luego de conocer el alcance de la infección, se podrá determinar si información sensible o equipos críticos se han visto afectados. En función de este resultado, se podrán tomar decisiones para continuar correctamente con las operaciones de la compañía.

Por otro lado, si la infección derivara en una fuga de información que puede comprometer datos de empleados, usuarios o clientes, será necesario contactarlos para avisar sobre la posible brecha; de esta manera, se podrá mantener el registro de cualquier movimiento de datos vinculados a los servicios proporcionados por la empresa.

En el caso de que algún equipo físico haya resultado comprometido, se deberán poner en marcha procesos de restauración de información y de los equipos de cómputo necesarios, a fin de mantener los servicios ofrecidos a clientes y usuarios. Por esto, resulta de vital importancia la planificación de defensas contra amenazas que atentan contra la disponibilidad, en estos casos pueden ser necesarios respaldos de infraestructura tecnológica y de información.

Las actividades están estrechamente ligadas con el contenido de un Plan de Continuidad del Negocio (mejor conocido como BCP por las siglas en inglés de *Business Continuity Plan*), de manera que procesos sustanciales de la organización se mantengan disponibles, luego de recuperar y restaurar las actividades críticas del negocio en un tiempo prudente. Una vez que se hayan erradicado los códigos maliciosos y sus consecuencias, se podrá regresar a la normalidad de manera progresiva.

3.4. Contener las acciones maliciosas

Las estrategias de contención pueden variar en función del incidente y de los lineamientos establecidos por los equipos de respuesta, lo que a su vez depende del tipo de *malware* que afecte a la organización. Por ejemplo, si un equipo se ve afectado por un caso de *ransomware*, se deberá seguir una estrategia distinta a si se está ante un caso de una *botnet* o un *spyware*. A partir del comportamiento del código malicioso se pueden determinar los pasos a seguir para la contención.

Una manera de iniciar esta fase está relacionada con el aislamiento de los equipos que se sabe que están comprometidos. La suspensión de los segmentos de red de los cuales forman parte evita que la infección pueda propagarse a través de la red corporativa e interrumpe cualquier conexión que pueda establecerse con el atacante para el robo de información. La segmentación de las redes es una práctica que contribuye a mitigar la propagación.

Por otro lado, la identificación del vector de ataque resulta fundamental para contener los estragos generados por un código malicioso y evitar su propagación. En este sentido, es importante la previsión para manejar incidentes que utilizan los vectores más comunes: propagación e infección a través de medios externos y removibles, explotación de vulnerabilidades en el *software* y sitios *web*, archivos adjuntos a correos electrónicos y enlaces a sitios que alojan *malware*.

Las ataques por *malware* pueden deberse a una campaña masiva de propagación que infectan los equipos de manera casual, quizá por malas prácticas de los usuarios, o bien puede tratarse de un ataque dirigido y con un propósito específico. En todos estos casos, una vez que se haya identificado el vector de ataque, se podrán aplicar distintas acciones en función de las características de la muestra de *malware*.

Por ejemplo, si se trata de un programa malicioso que realiza conexiones a Internet, con el monitoreo de los canales de comunicación de los atacantes se puede obtener el tráfico generado por el agente malicioso. En caso de que se encuentre cifrado, los analistas deben aplicar ingeniería inversa para intentar obtener las claves criptográficas que permitan el descifrado. En cambio, si la comunicación se realiza sobre protocolos no cifrados (como HTTP), será relativamente más sencillo realizar el seguimiento de los comandos utilizados por los ciberdelincuentes.

Asimismo, el análisis de los comandos puede guiar la investigación al descubrimiento de nuevos equipos infectados, mientras que la generación de patrones de tráfico (lo que debe traducirse en la creación de reglas de *firewall* para generar una primera barrera de defensa) permite bloquear los acciones que intente realizar cualquier agente malicioso que haya logrado saltar los mecanismos de seguridad.

En cambio, si se trata de una muestra de *malware* de la familia *Win32/FileCoder*, es decir, *ransomware* que cifra archivos, será necesario aplicar algún método de restauración de información con la intención de evitar el pago de la información secuestrada y mantener las actividades críticas.

De la misma manera, es necesario emitir las alertas necesarias al personal idóneo para mitigar la reproducción de los códigos maliciosos, ya sea que puedan presentarse por dispositivos removibles, correos electrónicos o cualquier otro medio de propagación.

La mayor parte de los procedimientos nombrados implican el análisis no automatizado de la información, por lo que se torna evidente que la prevención y detección proactiva de amenazas son la piedra angular de la Seguridad de la Información. Además, el desempeño de estas actividades tiene como propósito mantener los sistemas seguros, trabajando correctamente y evitarán que haya que recurrir a los Planes de Respuesta a Incidentes.

3.5. Erradicar la infección y eliminar el vector de ataque

La remoción de la amenaza es un procedimiento complejo que implica, inicialmente, un análisis minucioso del comportamiento del *malware* para comprender su funcionamiento y, en condiciones ideales, un análisis del código fuente del mismo. Las soluciones de seguridad dan soporte a este tipo de actividades, permitiendo la automatización de la desinfección y el ahorro de tiempo en el proceso de respuesta.

Si los medios empleados por los atacantes no son erradicados completamente, existe una enorme posibilidad de que puedan retomar sus actividades maliciosas sobre los equipos infectados a través de otro vector de ataque. Por ello, es de vital importancia aislar la falla que les permitió el ingreso, para luego eliminarla del sistema.

Aun si los equipos comprometidos han sido desinfectados, continúa presente el riesgo de mantener en funcionamiento otros equipos infectados no descubiertos. Para evitar que esto ocurra, se pueden poner en práctica otras acciones como el análisis de los paquetes de red para identificar tráfico anormal, con la ventaja de que ahora se conocen los protocolos, puertos y comandos utilizados en el análisis previo. Por lo tanto, todas las acciones de análisis son fundamentales para conocer el *malware* y, posteriormente, erradicarlo.

Luego de conocer el comportamiento, es necesario comenzar a aplicar medidas de protección. Por ejemplo, junto con la revisión de las reglas de *firewall*, el cambio de las contraseñas es otra medida preventiva a tomar luego de detectar recursos comprometidos, ya que éste es uno de los objetivos en los ataques corporativos. Si bien el proceso de actualización de credenciales de acceso implica dedicar tiempo y esfuerzo, impedirá que los atacantes puedan utilizar cualquier información robada para suplantar la identidad de un usuario legítimo.

De la misma manera, existen otras herramientas de seguridad, como los sistemas de 'Información de seguridad y administración de eventos' (SIEM por las siglas de *Security Information and Event Management*) o 'Sistemas de prevención y detección de intrusos' (IPS/IDS), que permiten contar con alertas tempranas sobre actividades anormales en la red y sistemas, y pueden ser configuradas para evitar nuevas infecciones que utilizan vías conocidas.

A partir de la identificación del método de propagación, es obligatorio llevar a cabo algunas acciones que mitiguen de manera específica el vector, por ejemplo el filtrado de correo electrónico y análisis de los mensajes y adjuntos, la modificación de los sistemas operativos para evitar la ejecución de programas de manera automática cuando se introduce un dispositivo removible, la actualización de *software* necesario para evitar la explotación de alguna vulnerabilidad que permita el ingreso de *malware* a la red corporativa, entre otras acciones.

Llegada esta instancia, es necesario definir si la infección fue el simple resultado de un descuido en la *Web* o si, por el contrario, constituye el eslabón exitoso dentro de una cadena de ataques persistentes y dirigidos. Si se determina que la infección tuvo como objetivo específico a la organización, entonces se debe tener en mente que un nuevo ataque puede ser inminente.

Por ello, el análisis de las piezas maliciosas debe orientarse a determinar las acciones específicas del *malware*, cómo puede ser detectado en la red, así como también medir y contener su daño. Una vez logrado esto, se deben generar las firmas correspondientes para detectar las infecciones en las redes corporativas. Gran parte de esta actividad puede ser realizada por los laboratorios de investigación.

3.6. Recuperar la normalidad en las operaciones

La fase de recuperación se presenta luego de que un incidente por *malware* ha sido contenido y de que se han identificado y mitigado las vulnerabilidades que fueron explotadas.

Llegado este punto, se confirma que los sistemas se encuentran funcionando de manera normal y que el *malware* ha sido removido para evitar incidentes similares. La recuperación puede incluir acciones como la restauración de sistemas operativos y respaldos, el reemplazo de archivos infectados, la instalación de parches de seguridad y actualizaciones, el cambio de contraseñas en los sistemas, el refuerzo de la seguridad perimetral a través de nuevas reglas de *firewall*, la creación de listas de control de acceso o el desarrollo de nuevas firmas de *malware*.

A partir de los patrones identificados, es posible determinar que si un ataque cumplió su cometido malicioso y si se intentarán nuevos casos de una manera similar. Por este motivo, es fundamental eliminar de raíz los problemas para mantener la seguridad; cabe destacar que esto logra con el conocimiento pleno del código malicioso.

El tiempo de recuperación dependerá en gran medida de las consecuencias generadas por la infección, por lo que no se puede establecer un periodo para alcanzarla, aunque siempre se busca que sea en el menor tiempo posible.

3.7. Registrar las lecciones aprendidas

Finalmente, otro elemento de importancia en el proceso de atención a incidentes es el aprendizaje y la mejora continua. Realizar una investigación de lo acontecido permite mejorar los procesos dentro de la organización y que los equipos de respuesta evolucionen para enfrentar nuevas amenazas.

El análisis puede llevarse a cabo por el personal interno encargado de atender las incidencias, o bien mediante el contacto con equipos especializados en el tema, por ejemplo, laboratorios de análisis en la región, como el de ESET Latinoamérica.

Con la investigación y posterior mitigación de vulnerabilidades que eran desconocidas, surge la oportunidad de fortalecer el perímetro de las redes y de identificar otros potenciales puntos de acceso a los sistemas que antes no habían sido considerados.

Las infecciones, a pesar de constituir eventos inesperados e indeseados para una compañía, también son situaciones de aprendizaje, ya que contribuyen a mejorar las medidas de seguridad y los procesos de atención de incidentes, muestran cuáles son los puntos a fortalecer dentro del diseño del sistema y permiten probar dónde fallan las medidas de defensa actuales, por lo que múltiples incidentes pueden ser prevenidos con una lección bien aprendida.

4. Medidas de seguridad ante incidentes por *malware*

Es evidente que el *malware* ha estado presente en la escena tecnológica por muchos años; además, los datos y hechos de la actualidad permiten pronosticar que seguirá viviendo y hasta evolucionando. Es importante, entonces, considerar esta información y entender que la sofisticación de los programas maliciosos tiene que ser una variable a considerar.

A pesar de ello, los vectores de ataque utilizados para propagar e infectar continúan siendo los que se observan hace tiempo, permitiendo que con el uso de herramientas de seguridad y buenas prácticas, una cantidad importante de programas maliciosos puedan ser descartados.

En este sentido, la principal perspectiva consiste en aplicar medidas preventivas y proactivas que brinden protección. Es fundamental contar con acciones que determinen lo que se debe hacer antes de que ocurra un incidente. Si bien esto es lo ideal, puede que estas medidas sean sobrepasadas, por lo que también es importante contar con un Plan de Respuesta a Incidentes con una lista de acciones a ejecutar durante una infección maliciosa y posterior a la misma. Por ello, es necesaria una combinación de herramientas tecnológicas, buenas prácticas y gestión de la seguridad.

Imagen 5. Combinación de tecnología, buenas prácticas y gestión para proteger la información y el negocio.

Entre las principales herramientas y prácticas de prevención se encuentra la correcta implementación de una solución de seguridad contra *malware* (antivirus), así como otras herramientas de detección temprana de amenazas. De la misma manera, actividades como la actualización del *software* o el respaldo de la información (*backup*), son fundamentales para reducir las consecuencias negativas generadas por un ataque de *malware*.

Además, son necesarias otras prácticas, como la educación y concientización de los usuarios en temas de seguridad. Hay distintas opciones al alcance de las organizaciones con capacitaciones especializadas, como ACADEMIA ESET que ofrece cursos y carreras en una plataforma en línea.

De la misma manera, es vital mantenerse actualizados en las últimas noticias de seguridad para conocer alertas, nuevas amenazas y vulnerabilidades descubiertas. Una opción es *WeLiveSecurity en español*, el portal de noticias, opiniones de expertos e investigación de seguridad informática de ESET.

Con estas y otras fuentes de información, se podrán conocer las principales vías de ataque de los cibercriminales y la forma en la que las organizaciones pueden verse afectadas, pero sobre todo se podrá ver lo que sus integrantes pueden realizar para evitarlo. Estos recursos pueden ser incluidos en campañas de concientización que, sin duda, contribuyen a evitar los incidentes relacionados con códigos maliciosos.

En este conjunto de medidas preventivas y reactivas, no se debe dejar de lado la gestión, tanto de las herramientas tecnológicas (que incluyen su instalación, configuración y actualización), como del personal de las organizaciones, con prácticas como el desarrollo y aplicación de políticas de seguridad, las campañas de concientización y capacitación ya mencionadas, así como la alineación con estándares de seguridad.

Ante cualquier incidente relacionado con *malware* se puede recurrir a equipos especializados en el análisis y respuesta a infecciones, como el Laboratorio de ESET que ofrece consultas especializadas a través del soporte técnico para empresas.

5. ¿Qué hacer con muestras capturadas luego de una infección?

Con el propósito de ofrecer productos efectivos a los usuarios, ESET poner a disposición un canal de comunicación donde se pueden enviar muestras de virus y otros códigos maliciosos para su análisis. Para hacerlo, se deben seguir los pasos descriptos a continuación.

5.1. Manejo y envío de muestras al Laboratorio de ESET

Si se ha presentado un comportamiento sospechoso o actividades maliciosas en un sistema y es posible determinar el programa que lo ha generado, la muestra de *malware* puede ser enviada al Laboratorio de análisis de *malware* de ESET a través de correos electrónicos con los siguientes pasos:

a) Comprimir el/los archivo/s sospechoso/s en formato ZIP o RAR, y protegerlo con la contraseña "*infected*", sin comillas (es recomendable no enviar más de diez muestras por correo).
b) Anotar la mencionada contraseña en el correo, adjuntar el archivo comprimido y enviarlo a samples@eset-la.com.
c) Indicar en el asunto y en el cuerpo del correo si el archivo adjuntado contiene una muestra de virus o un falso positivo (ejemplo: utilizar el asunto 'Infección sospechosa' o 'Falso positivo' si se informa sobre un falso positivo).
d) Si se desea informar sobre un sitio *Web* bloqueado que podría incluir contenido potencialmente peligroso, se puede dirigir el correo a la dirección samples@eset-la.com, pero el asunto deberá contener la leyenda 'Dominio Sospechoso' seguido del dominio bloqueado. No se debe escribir la dirección URL completa en el asunto (ejemplo: www.dominiobloqueado.com/pages/index.htm), sino solamente el dominio propiamente dicho (ejemplo: www.dominiobloqueado.com).
e) En el cuerpo del mensaje del correo es importante detallar:

- Cualquier antecedente relacionado con el origen de la muestra.
- Cantidad de equipos afectados.
- Motivo por el cual se cree que se trata de un código malicioso o un falso positivo.
- Si se conoce otra solución antivirus que actualmente detecta la amenaza (especificar).
- Si se informa un falso positivo, es importante proporcionar la mayor cantidad de información posible acerca del *software*, incluyendo nombre del fabricante, nombre y versión de la aplicación y la dirección del sitio web desde la cual se descargó el archivo.
- Si se informa sobre un sitio *Web* bloqueado, se deberá precisar la dirección URL implicada de manera completa. Es recomendable adjuntar una captura de pantalla en la que se visualice la notificación de bloqueo.

5.2. Envío de muestras al Laboratorio de ESET

El proceso de envío de muestras al Laboratorio se puede realizar directamente desde la solución:

a) Dirigirse a la sección 'Herramientas' y elegir la opción 'Enviar el archivo para su análisis'.

Imagen 6. Interfaz de ESET Endpoint Security para el envío de muestras de malware *– Paso 1.*

b) Luego, indicar el motivo por el cual se envía un archivo (archivo sospechoso, falso positivo u otro) y especificar la ruta del archivo. De manera opcional, se puede incluir una dirección de correo electrónico de contacto en caso de se requiera más información.

Imagen 7. Interfaz de ESET Endpoint Security para el envío de muestras de malware *– Paso 2.*

c) Incluir información adicional que permita realizar una descripción del archivo:

- Signos y síntomas observados de infección de malware. Ingresar una descripción sobre la conducta de los archivos sospechosos observada en el equipo.
- Origen del archivo (dirección URL o proveedor). Ingresar el origen del archivo (la procedencia) e indicar cómo se lo encontró.
- Notas e información adicional. Ingresar información adicional o una descripción útil en el proceso de identificación del archivo sospechoso.

Aunque solo el primer parámetro (Signos y síntomas observados de infección de *malware*) es obligatorio, el suministro de información adicional ayudará en forma significativa en la etapa de identificación y en el procesamiento de muestras.

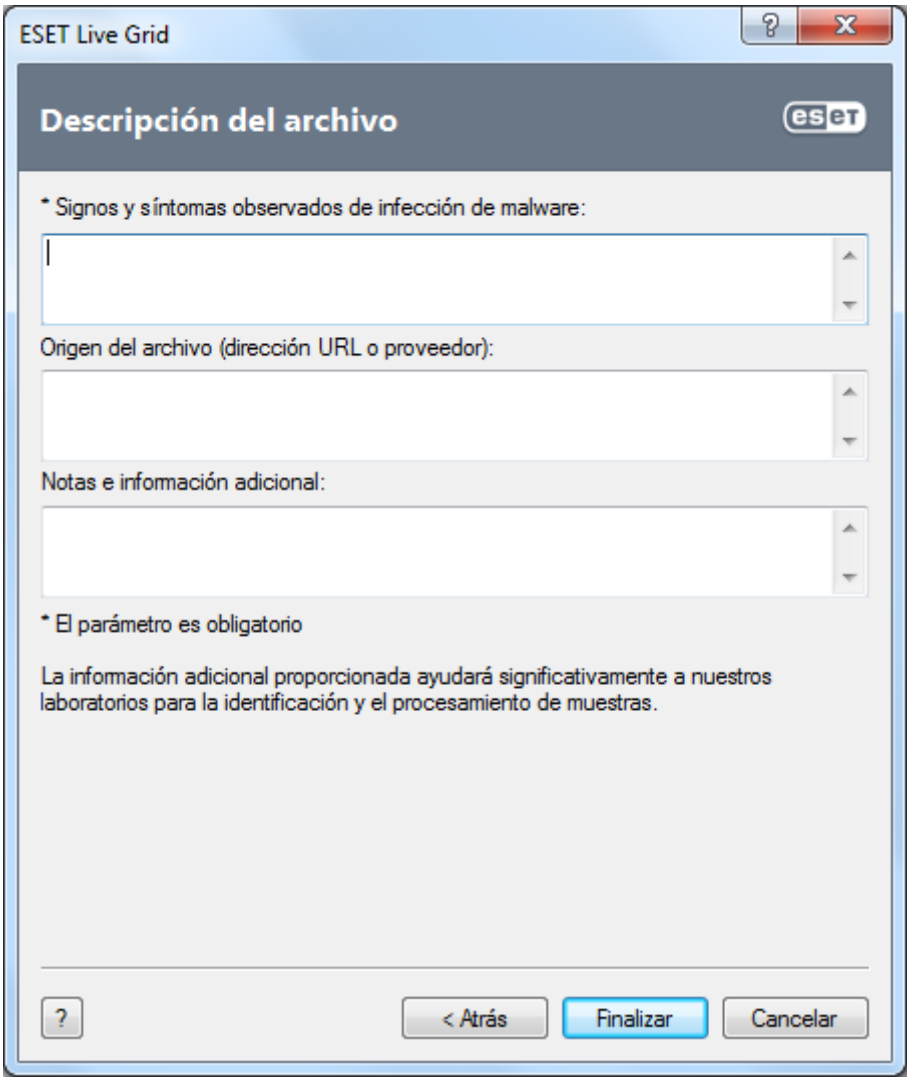

Imagen 8. Interfaz de ESET Endpoint Security para el envío de muestras de malware *– Paso 3.*

6. Conclusiones

Esta guía general sobre los pasos a seguir en caso de una infección por *malware* tiene como propósito contribuir a reducir las incidencias causadas por códigos maliciosos dentro de las organizaciones. Al mismo tiempo, intenta acompañar al personal preocupado en la protección de la información, para definir un plan de acción en caso de que la infección se presente, de manera que el impacto sea mínimo y pueda garantizarse la continuidad de las operaciones críticas del negocio.

A través de la definición de actividades y funciones en cada una de las fases, se pretende que la respuesta a incidentes de seguridad de esta naturaleza sea efectiva y en el menor tiempo posible. Por ello, se han considerado fases que parten desde la identificación y determinación del alcance de una infección por *malware*, la continuidad de operaciones críticas, contención de las actividades maliciosas, erradicación de la infección y del vector de ataque, recuperación de la normalidad en las operaciones, y hasta el registro de lecciones aprendidas.

De la misma manera, se resalta la importancia del uso de la tecnología de seguridad, aplicada en medidas de protección preventivas, proactivas y reactivas. Por lo tanto, esto considera la combinación de soluciones tecnológicas, buenas prácticas y la gestión de Seguridad de la Información.

ESET desarrolla soluciones para estos propósitos, que incluyen tecnología de seguridad, materiales educativos y de concientización, aunado a la investigación en materia de amenazas informáticas. Al mismo tiempo, pone todos estos recursos a disposición de las empresas que los requieran para aumentar y mejorar su seguridad, de modo que puedan hacer más, proteger sus activos y lograr sus objetivos.

7. Referencias

7.1. Publicaciones en *WeLiveSecurity* en español

http://www.welivesecurity.com/la-es/2015/03/05/5-pasos-tras-infeccion-empresa/

http://www.welivesecurity.com/la-es/2012/03/13/consejos-controlar-infeccion-malware/

http://www.welivesecurity.com/la-es/2011/02/25/me-infecte-y-ahora-que-hago-parte-i/

http://www.welivesecurity.com/la-es/2011/03/03/me-infecte-y-ahora-que-hago-parte-ii/

7.2. Artículos en la base de conocimientos (ESET *KnowledgeBase*)

Reporte de códigos maliciosos a nuestro laboratorio:

http://www.eset-la.com/soporte/muestras

¿Cómo enviar muestras de malware, sitios *web* o falsos positivos a los laboratorios de ESET?

http://soporte.eset-la.com/kb141

7.3. Informes de seguridad ESET Latinoamérica

http://www.welivesecurity.com/la-es/articulos/reportes/